

Discovering Unburied Treasure on Social Networking Websites

By *Rubin M. Sinins, Newark, NJ*

My attorney father was mortified when I declared in 1992 that my classmates and I could obtain access to people's real estate records. With a database password and a computer, these financial secrets were ours. When I pointed out that this information was public, my father's response illustrated the tension between our *ability* to access personal information and the *appropriateness* of doing so. "Even public information can be personal and should be kept private," he said. "It shouldn't be so easy to learn people's business."

That was just the beginning of computerized information. In 2009, seeking information on the Internet has become the norm rather than the exception. But nearly two decades later, with a fully blossomed Internet, my father's wisdom remains valid. Today, attorneys struggle with this same tension. The line between private and public information is being erased.

Recent advances in technology make my father's concern over property records seem quaint. Today, just about anything can be learned with an Internet connection and search tools. Perform a Google or Yahoo! search of your own name. You will be amazed at the results. You will quickly realize that data you *believed* to be private is actually *publicly available*.

Background to Web 2.0:

The Internet as a Platform

The Internet has evolved and Web sites are no longer static destinations. Even sites that remain constant—your law firm's site, for example—now contain updated functionality. This "platform functionality," which permits users to interact and to accomplish tasks, distinguishes today's Internet from earlier versions.

This new Internet functionality has been called "Web 2.0."¹ Although the phrase has different meanings and is a source of some debate, the underlying concept is that the World Wide Web can be a platform to get things done.² So instead of purchasing software for word processing or other jobs, one uses applications already built into sites. Content is available online and does not need to be downloaded.³

Social interaction is a cornerstone of Web 2.0. With today's sites, you can network, share information, communicate, create blogs, "tag" and share site addresses, and interact in other innumerable ways. Web 2.0 sites offer web-based tools for all these pursuits. The hub of Web 2.0 social interaction revolves around social networking Web sites (SNW).⁴

What are SNWs? They are services dedicated to information-sharing among groups and individuals with common interests. SNWs provide users with a variety of ways to communicate, including e-mail and instant messaging. SNW users create profiles for themselves, join groups, and link to each other as online "friends."

Because SNWs encourage users to reveal a remarkable amount of personal data, they are a treasure trove of personal information. User "profiles" can include "About Me" posts as well as blogs; friends; favorites (music, books, movies); education; employment; posts (typed messages or taglines); photos; videos; and other data.⁵ Messaging is universal; users can post comments about their status and comment on the status of others.⁶ In this virtual world, you can maintain a full online identity linked to others.

But what about privacy? Theoretically, both "private" information and "public" information exists on SNWs. Users can adjust the level of personal information available to

others by choosing among various privacy settings.⁷

For example, there may be a limited “public” profile and more complete information available to “friends.” Even “friends” may be blocked from certain information. In short, there are varying levels of privacy. The extent of shared information depends on users’ choices as well as on the content disseminated through messaging and posts over an SNW.⁸ When users routinely shares information over an SNW, maintaining privacy may be difficult, even when they take advantage of the privacy controls.

Moreover, profiles can be partially available even outside the SNW. Information is usually publicly available through search engines such as Google. Even more significantly, notwithstanding privacy settings, every bit of SNW account information may be sought, and possibly obtained, through the litigation discovery process. And once a recipient obtains that previously private information, there is little to no control over its use and distribution.

The Legal Battle over Private vs. Public Information

Can information published over the Internet ever maintain its status as a private record? That is the conundrum we face as society uses the Internet as the primary mode of communication. It is a problem of special concern to litigators.

SNWs will loom large in upcoming discovery battles. Litigating in the age of Web 2.0 requires you to increase your technical knowledge. As a litigator, you had better understand SNWs. Every case you are handling—civil or criminal—could potentially benefit or suffer from information on an SNW. What is more, you can be sure your adversaries understand SNWs. They are salivating at the opportunity to harness this new investigative tool to destroy your case.

But have no fear. You likely already know about the more popular SNWs. In the United States, Facebook and MySpace dominate the market. Facebook boasts more than 150 million active users.⁹ In 2006, there were more than 100 million MySpace users.¹⁰ Besides these market leaders, many more SNWs exist and are created each month.

Why are SNWs so popular? SNW membership is free, easy, fun, and an extremely efficient way to communicate and develop an Internet presence. You can debate the usefulness of SNWs, but you cannot debate that SNWs are the dominant mode of social interaction for today’s youth and, increasingly, for older adults as well.

You should join the world of SNWs. At the very least, your experience will educate you about their workings and their scope.

Get Ready: Here They Come

How will this knowledge help your practice? Defense counsel is already preparing to exploit the latest technological tools against your clients. We are all familiar with traditional defense surveillance techniques. An investigator will follow a plaintiff in an attempt to record activities inconsistent with alleged disabilities. Nothing is more devastating than a video recording an allegedly disabled plaintiff playing pickup basketball, swimming, or golfing.

Internet communications, including SNWs, alter investigative strategy. In many respects, they make surveillance unnecessary. Plaintiffs may be creating their own evidence to undermine their cases and their “electronic footprints” may be used against them. You must be prepared to guard against this eventuality.

Every defense counsel has a “treasure map” to unearth damaging evidence that is better left buried. Recent articles published by the defense bar have urged counsel to consider the

following SNW discovery methods: (1) using search engines to discover a plaintiff and witness's Internet activities; (2) demanding identification of e-mail accounts; (3) investigating whether a plaintiff uses an SNW; (4) viewing and analyzing public portions of an SNW; (5) demanding production of the contents of an SNW, including private areas, such as messaging; identifying witnesses from a plaintiff's SNW "friends"; (6) demanding that an SNW prevent deletion of a plaintiff's account information; (7) consenting to a protective order as a condition of production; and (8) seeking *in camera* review of the contents of an SNW to explain the relevance of the SNW data to the issues in the case.¹¹ One defense blogger urged counsel to bring a computer with Internet access to the plaintiff's deposition. Counsel would then request that the plaintiff log onto his SNW and provide a tour of the account for defense counsel!¹²

Are these approaches unrealistic, scorched earth defense tactics? Or are they a preview of standard discovery techniques to come? Welcome to discovery battles in a Web 2.0 world.

Something (You Didn't Know) about Mary: A Hypothetical

Typically, SNW discovery disputes will arise in the civil context. Although criminal cases involve similar issues, the pre-indictment criminal process (e.g., warrants, administrative and grand jury subpoenas) is generally *ex parte*. There is, accordingly, little opportunity to challenge disclosures by SNWs until after they are made. Let's take a practical walk through a hypothetical civil matter and put our knowledge into practice.

In our civil matter, you are the plaintiff attorney representing Mary, a 17-year-old high school senior. Mary has sued her school district and others due to emotional distress caused by a sexual relationship instigated by her 35-year-old English teacher, beginning when she was 14. Psychiatric reports confirm post-traumatic stress disorder. The case is defended by a young upstart from a respected and aggressive firm.

You are far from a novice and intend to be thorough. From the start, you explored with Mary the potential for embarrassing evidence. She confirmed there were no e-mails between her and the teacher. The pedophile was paranoid about being discovered. There were likewise no text messages. Cellular phone records revealed hundreds of calls between them, but those records do not reveal the *content* of the calls. The defense serves discovery demands. They ask for all the e-mail addresses Mary has used. You disclose the two accounts Mary has used since she was 13. You are confident there are no harmful communications to be discovered. Within days, your confidence has shattered. The defense has filed for a commission to seek discovery from California-based Facebook and MySpace. Defense counsel is seeking the complete content of Mary's accounts, including all private messages.

Do Not Panic: Understand and Explain

How did the defense even know that the plaintiff utilized those SNWs? It turns out Mary's Facebook public profile appeared through a simple Google search. She had not blocked it through privacy settings. The computer-savvy defense counsel—as a subscriber to Spokeo.com, a search service—entered Mary's disclosed e-mail addresses and found she was a MySpace user as well.¹³ Indeed, the Spokeo Home Page boasts, "uncover personal photos, videos, and secrets...GUARANTEED."¹⁴

Shaken, you meet with your client. You tell her about the commission application. Mary begins to squirm. Brief inquiry reveals that Mary is an extremely active Facebook and MySpace user. More to the point, she admits that her "whole life" is on these SNWs. For obvious reasons,

she would rather not have disclosed her messages with “friends,” particularly those with her new boyfriend. She insists that her SNW accounts are private. She insists you make this “go away,” or she will abandon her case. Her parents, dumbfounded, ask you to explain how this could be happening. “Don’t we have rights?” they ask.

General Principles of Privacy Law

The correct answer to that question is: “Yes and no.” You would be mistaken to assume Mary has firmly established privacy rights in her SNW accounts.

Constitutional Privacy Rights?

As a constitutional matter, it is likely that Mary has no protected privacy interest in SNW-held information. Under the Fourth Amendment to the Constitution, one has no expectation of privacy in information held by third parties.¹⁵ It has been uniformly held under federal law that there is no constitutional privacy interest in the information held by Internet service providers (ISP).¹⁶ Most state constitutions follow the federal standard.¹⁷ The only exception is New Jersey, where a state constitutional privacy right exists.¹⁸ Moreover, you are involved in a private civil matter, not a criminal case; it is often an open question whether state constitutions protect against private, as opposed to “state,” action.

Internet privacy rights are typically analyzed in the context of *anonymous* internet activities. Many Web 2.0 blogs permit users to contribute anonymously through the use of pseudonyms. Constitutional protection does exist for certain anonymous web postings.¹⁹ The issue arises when others claim that the pseudonymous web user has broken the law or otherwise infringed their rights. Then courts have been asked to permit the ISP to reveal customer information.²⁰ That information discloses the name of the previously-anonymous user. Standards have emerged for weighing the privacy right against the need for disclosure.²¹ Mary, however, has not been posting anonymously.

Statutory Privacy Rights?

As a statutory matter, Mary has limited protections. Federal and state wiretap statutes protect ISP-held information.²² Court orders, warrants, or grand jury subpoenas are required to trump that privacy interest.²³ But those requirements pertain only to law enforcement. Here a civil subpoena is threatened. It is unclear if civil subpoenas must be honored. This writer is unaware of any statute barring disclosure of SNW account information in response to a civil subpoena. The existence of wiretap statutes regulating law enforcement has not been found implicitly to preclude civil process.

Contractual Privacy Rights?

As a matter of contractual rights, Mary’s privacy rights are extremely limited. Typically an SNW provides “Terms of Use” and “Privacy Policies” for users.²⁴ These agreements provide that user information is generally private; however, SNWs, including Facebook, warn that the disclosure of personal information may lead to the information becoming publicly available. Invariably the SNW policies further provide that the SNW shall disclose user information pursuant to lawful process, including court orders. It could hardly be otherwise. To this writer’s knowledge, no SNW has taken the position that it shall defy court disclosure orders.

Privacy under Decisional Law?

As a matter of common law, there are no controlling decisions from federal or state courts addressing this issue. There is little case law on SNW discovery.

Adam Slater, an AAJ member and New Jersey attorney, recently had success in prohibiting the release of SNW information in an emotional distress case. Slater's client, a minor, was sexually assaulted by a fellow student. In *T.V. v. Union Township Board of Education*, Slater argued that protections are especially important in cases involving minors. "[T]he minor plaintiff has relied on the ability to communicate confidentially with her friends, via the Internet, just as she would have by telephone."²⁵

The Court agreed, at least to a point; it required the defense to engage in traditional discovery techniques before seeking the Plaintiff's private SNW messages. While the Court permitted the defense to renew its application if it could show a particular need, the defense never did so.²⁶

In the only SNW discovery decision of its kind located on Westlaw, a Nevada federal court, in an "unreported" decision, also rejected a defense effort to obtain a plaintiff's SNW information. In *Mackelprang v. Fidelity National Title Agency of Nevada, Inc.*, a sexual harassment case, defendant sought disclosure of two MySpace accounts, along with the disclosure of all private messages on the accounts.²⁷ Although the plaintiff did not admit the accounts belonged to her, evidence strongly suggested they did. The defendant claimed the messages were relevant to reveal: (1) consensual sexual relations with other MySpace users; (2) discussions about the case that would thereby constitute relevant admissions; and (3) evidence that plaintiff's emotional distress was caused by other factors.²⁸

The court rejected the discovery application as a "fishing expedition," based on nothing more than speculation about the messages' contents.²⁹ The court noted, however, that its order did *not* prevent the defendant from serving upon the plaintiff demands that she produce all relevant messages from her MySpace accounts.³⁰ Defendant was also *not* prohibited from conducting discovery to prove the accounts were, in fact, the plaintiff's.³¹ MySpace had produced the "public" portions of the account in response to the subpoena.³²

In a different context, a New Jersey federal court rejected the plaintiffs' arguments for a protective order to preclude SNW discovery. *Beye v. Horizon*³³ and *Foley v. Horizon*³⁴ were challenges to a health insurer's refusal to pay benefits for children's eating disorders. The court required plaintiffs to produce writings that were "shared with other people," about the disorder, including messages on SNWs, such as Facebook and MySpace.³⁵ The court apparently drew the line between private and public information at the point of shared communication.

Entering the Fray: Seeking Protection from Disclosure

So Mary's privacy interests are not entirely established or self-enforcing. What is to be done? You must seek a protective order denying the commission and prohibiting the requested discovery of SNW information.

But you will be faced with broad discovery rules which permit discovery of any information that may lead to the disclosure of admissible evidence.³⁶ Defense counsel will claim Mary's communications over the SNWs are relevant to her emotional condition. After all, the argument will go, Mary has placed her condition in issue, and thereby waived any privacy interest in such information. What better evidence of Mary's state of mind than her unguarded communications? The defense shall further argue that SNW users' privacy rights are no greater

than those of e-mail users. Relevant e-mail is routinely discoverable.

Your application for a protective order should highlight the significant invasion defendants are proposing. SNWs are today's method of communications. In less technologically sophisticated times, the contents of telephone calls could never have been retained, much less disclosed. A discovery request for SNW information is tantamount to a retroactive wiretap. The *contents* of communications merit the most privacy protection.

The defense's request also ignores the chilling effect such ordered disclosure would have. The discovery demand is nothing more than a fishing expedition. What is more, the defense casts a wide net without knowing or identifying the relevance of any messages or other content. You must insist that a particular need be shown before disclosure is ordered, and that the defendant establish the information cannot be obtained elsewhere. Otherwise SNW disclosure motions will be made in every case.

If any disclosure is to be considered, you must seek *in camera* inspection of the materials for disclosure only of relevant portions. Alternatively, you should seek SNW production to *you* for production to the defense only of relevant information.

Lessons to Be Learned in Protecting Information

Much can be learned from Mary's hypothetical dilemma. It is better to prevent such problems than to cure potentially devastating disclosures after they are revealed. It is important that the following steps be implemented:

- Clients must be advised not to use SNWs during the pendency of your representation
- If SNWs must be used, the highest privacy settings should be chosen and password protected; only the most limited and trusted "friends" should be linked, and no compromising material or messages should be posted or otherwise shared
- Any prior content of the SNW should be reviewed thoroughly, to understand any possibly negative evidence that may be discovered
- Clients should be advised that, in today's litigation environment, the boundary between private and public data is unclear and ever-changing; they should never assume that any statement or action will remain confidential
- Clients should be advised that the consequences of embarrassing disclosures may be the loss of credibility or even the loss of their claims

Remaining on the Offensive

Remember that we represent victims. When we file suit, the defense often engages in a no-holds-barred quest for damaging information. But we must always bear in mind that we are the ones who are damaging them with legitimate complaints about improper conduct. Defendants are the tortfeasors. They are responsible to account for their actions.

Discovery is a two-way street. Nothing prevents the plaintiff from seeking additional evidence against the defendants. Is it inconceivable that defendants would make embarrassing admissions on an SNW? We often find the "smoking gun" in unguarded e-mail communications. Keep in mind that defendants' SNW information may be a treasure trove for us as well.

Trial Considerations

What happens if you lose the discovery motion and the SNW data is disclosed? Then you

must fight to preclude its use at trial.

There is a big difference between discovering information and entering it into evidence. Trial evidence must be both *relevant*³⁷ and *admissible* under the operative Rules of Evidence. Admissibility will also depend upon whether the evidence is *authenticated*.³⁸ Its *prejudicial nature* also must not outweigh the *probative value* in its introduction.³⁹

SNW information may or may not meet those requirements. The federal decision in *Lorraine v. Markel American Insurance Co.*⁴⁰ provides a thorough discussion of the Federal Rules of Evidence as they relate to the potential admissibility of electronically stored information.

The authenticity requirement is perhaps the most difficult obstacle for admissibility. It is possible to create electronic evidence in a name other than your own.⁴¹ A witness or litigant may attempt to deny authorship. That is what happened in *Mackelprang*,⁴² when the plaintiff did not admit the MySpace sites belonged to her. Authentication is met by evidence sufficient to establish that the evidence is what the proponent claims.⁴³ A proponent must present testimony about where the SNW data came from and who authored it. Remember that if authorship by a party-opponent can be established, it is an admission.⁴⁴

Other hearsay objections may be met through exceptions to the Hearsay Rule or because the information is not “hearsay.” Perhaps, for example, the evidence is not being admitted for its truth.⁴⁵

The admissibility of SNW information follows the same analysis as non-electronic evidence.⁴⁶ Keep in mind that the war against admissibility of SNW evidence is separate from the battle over initial disclosure. You may lose the battle, but win the war by preventing the use of SNW information at trial.

Beyond Litigation: Making Social Networking Websites Work for You

It remains to be seen whether attorneys will benefit from marketing on SNWs. Facebook and MySpace sell advertising, although legal advertising appears uncommon or non-existent.

However, attorney marketing on SNWs can reach beyond advertising. There is a growing attorney presence on SNWs. Attorneys throughout the United States have developed profiles as SNW users. Law firms also have profiles. It has been reported that SNW presence is “useful to enhance your professional image, expand your network and boost your visibility.”⁴⁷

Small law firms and solo practitioners can have equal or more dominant impact on SNWs as the large firms. Your profile and communications are limited only by your imagination. Sophisticated clients are researching their attorneys on the Internet. Professional and well thought out SNW identities establish you as a cutting-edge practitioner. It is beyond the scope of this article to discuss the state of existing legal social networking Web sites. For the more general SNW, however, your audience is the public at large. They are your potential clients. So put a professional face on Facebook or another SNW.

Whether or not you utilize an SNW to market your firm, these sites are extraordinarily useful to all litigators. SNWs are an online world covering all manner of information. Learning how to protect and access that data can make a significant difference in your skill level as you pursue justice for your clients.

07102; T: 973-642-7005; rsinins@javerbaumwurgaft.com; www.javerbaumwurgaft.com.

Mr. Sinins is a partner at Javerbaum Wurgaft Hicks Kahn Wikstrom & Sinins. He is certified by the Supreme Court of New Jersey as a Criminal Trial Attorney and is a member of the Court's Rules of Evidence Committee.

1. TERRY BURROWS, *BLOGS, WIKIS, MYSFACE, AND MORE: EVERYTHING YOU WANT TO KNOW ABOUT USING WEB 2.0 BUT ARE AFRAID TO ASK* 16-18 (Chicago Review Press 2007).
2. *Id.* at 17.
3. *Id.*
4. *Id.* at 18.
5. See e.g., <http://www.facebook.com> (user profiles contain these elements and more).
6. *Id.*
7. See, e.g., *Facebook Privacy Settings*, <http://register.facebook.com/editaccount.php?ref=mb>.
8. *Id.*
9. *Facebook Press Room*, <http://facebook.com/press/info.php?statistics>.
10. Pete Cashmore, *MySpace Hits 100 Million Accounts*, MASHABLE, Aug. 9, 2006, available at <http://mashable.com/2006/08/09/myspace-hits-100-million>.
11. Ronald J. Levine & Susan Swatski-Lebson, *Are Social Networking Sites Discoverable?*, LEGAL TECH., Nov. 13, 2008, available at <http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202425974937>; Benjamin Rolf, et al., *The Usefulness of Social Networking Websites to a Resourceful Defense Team*, Product Liability Committee Newsletter Strictly Speaking, Jan. 30, 2008, available at http://www.imakenews.com/prodliab/e_article001005443.cfm?x=bc5Shqq,b2qHJnqr.
12. James M. Beck & Mark Herrmann, *E-Discovery for Defendants*, Drug & Device Law, Feb. 14, 2008, <http://druganddevicelaw.blogspot.com/2008/02/e-discovery-for-defendants.html>.
13. See <http://www.spokeo.com>. The suggested use of Spokeo.com by defense counsel appeared in Daniel A. Schwartz, *Conducting Discovery in Discrimination Claims: Are Social Networking Sites Like Facebook Off-Limits or Untapped Treasure Trove?* Conn. Employment Law Blog, Nov. 13, 2008, <http://www.ctemploymentlawblog.com/2008/11/articles/hr-issues/conducting-discovery-in-discrimination-claims-are-social-networking-sites-like-facebook-offlimits-or-untapped-treasure-trove/>.
14. *Id.*
15. *Smith v. Maryland*, 442 U.S. 735 (1979); *California v. Greenwood*, 486 U.S. 35 (1988); *U.S. v. Miller*, 425 U.S. 435 (1976).
16. See *Guest v. Leis*, 255 F.3d 325, 335-36 (6th Cir. 2001); *U.S. v. Sherr*, 400 F. Supp. 2d 843, 848 (D. Md. 2005); *Freedman v. Am. Online, Inc.*, 412 F. Supp. 2d 174, 181-83 (D. Conn. 2005); *U.S. v. Cox*, 190 F. Supp. 2d 330, 332 (N.D.N.Y. 2002); *U.S. v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000); *U.S. v. Hambrick*, 55 F. Supp. 2d 504, 507-509 (W.D. Va. 1999).
17. *In re Property of Forgione*, 908 A. 2d 593, 607-08 (Conn. Super. Ct. 2006); *Hause v. Commonwealth of Kentucky*, 83 S.W. 3d 1, 25-29 (Ky. Ct. App. 2001).
18. *State v. Reid*, 945 A.2d 26 (N.J. 2008).
19. See, e.g., *Doe v. 2TheMart.com Inc.*, 140 F. Supp. 2d 1088, 1092, 1097 (W.D. Wash. 2001); *Dendrite Int'l, Inc. v. Doe No. 3*, 775 A.2d 756, 760 (N.J. Super. Ct. App. Div. 2001).
20. *In re Subpoena Duces Tecum to Am. Online, Inc.*, 2000 WL 1210372, at *6 (Va. Cir. Ct. Jan. 31, 2000); *Sony Music Entertainment, Inc. v. Does 1-40*, 326 F. Supp. 2d 556 (S.D.N.Y. 2004); *Immunimedics, Inc. v. Doe*, 775 A.2d 773 (N.J. Super. Ct. App. Div. 2001).
21. See, e.g., *Dendrite*, 775 A.2d at 760.
22. Title II, Electronic Communications Privacy Act of 1986, 18 U.S.C.A. §§ 2701-2712 (commonly referred to as Stored Communications Act); New Jersey State Wiretapping and Electronic Surveillance Control Act, N.J. STAT. ANN. § 2A:156A-29f. The author practices in New Jersey, so New Jersey Statutes and Court Rules are included, along with federal authorities.
23. 18 U.S.C.A. § 2703(c)(1); N.J. STAT. ANN. § 2A:156A-29a, e, f.
24. See, e.g., *Facebook Terms of Use*, <http://www.facebook.com/home.php#/terms.php?ref=pf>; *Facebook Privacy*

Principles, <http://www.facebook.com/php#/policy.php?ref=pf>.

25. Henry Gottlieb, *MySpace, Facebook Privacy Limits Tested in Emotional Distress Suit*, LAW.COM, June 14, 2007, available at <http://www.law.com/jsp/article.jsp?id=1181725536838>.

26. Telephone Interview with Adam Slater, Esquire, Mazie Slater Katz & Freeman (Feb. 2, 2009).

27. 2007 WL 119149, *2 (D. Nev. Jan 9, 2007)

28. *Id.* at *2-*8.

29. *Id.* at *7-*9.

30. *Id.* at *8.

31. *Id.*

32. *Id.* at *2.

33. 06-Civ. 5337 (D.N.J. 2006).

34. 06-Civ. 6219 (D.N.J. 2006).

35. Mary Pat Gallagher, *MySpace, Facebook Pages Called Key to Dispute over Insurance Coverage for Eating Disorders*, LAW.COM, Feb. 1, 2008, <http://www.law.com/jsp/article.jsp?id=1201779829458>.

36. FED. R. CIV. P. 26(b)(1); N.J. CT. R. 4:10-2.

37. FED. R. EVID. 401; N.J. R. EVID. 401.

38. FED. R. EVID. 901; N.J. R. EVID. 901.

39. FED. R. EVID. 403; N.J. R. EVID. 403.

40. 241 F.R.D. 534 (D. Md. 2007).

41. *St. Clair v. Johnny's Oyster & Shrimp, Inc.*, 76 F. Supp. 2d 773, 774-75 (S.D. Tex. 1999).

42. 2007 WL 119149 at *2.

43. FED. R. EVID. 901(a); N.J. R. EVID. 901(a).

44. FED. R. EVID. 801(d)(2); N.J. R. EVID. 803(b).

45. FED. R. EVID. 801(c); N.J. R. EVID. 801(c).

46. *Lorraine*, 241 F.R.D. at 538.

47. Sally Kane, *Using Social Networking Sites to Your Advantage*, About.com Guide to Legal Careers, Aug. 19, 2008, <http://legalcareers.about.com/b/2008/08/19/tuesdays-tip-use-social-networking-sites-to-your-advantage.htm>.